REMARKS

Reconsideration and allowance in view of the following remarks are respectfully requested.

Claim 1-33 remain pending for examination.

The following remarks address the claims in the order which they were addressed in the Office Action.

Rejections Under 35 U.S.C. §102(e)

Claims 12, 15, and **19** were rejected under 35 U.S.C. §102(e) as being anticipated by Ala-Laurila (U.S. Patent 6,704,789; hereafter "Ala-Laurila"). The Applicant respectfully traverses the rejection, and requests that this rejection be reconsidered and withdrawn. More particularly the Applicant submits that the rejection does not fulfill all of the requirements of MPEP §2131, which states, in part:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

The Applicant respectfully notes that **Claim 12** is an independent claim and the rejection of **Claims 12, 15, and 19** appear to actually be directed to independent **Claim 12**. Therefore, the Applicant will address the rejections to **Claim 12** first and the rejections to **Claims 15 and 19** immediately following.

In general, Ala-Laurila discloses using a subscriber identification module (SIM) to authenticate a user from a first network to a second data network. That is, Ala-Laurila is primarily directed to validating and identifying users consistently between a first network and a second data network. In contrast, **Claim 12** is directed, *inter alia*, to dynamically assigning internet protocol address to a wireless client over a secure link. In particular,

the authentication of a user and the establishment of one or more secure links are not analagous operations.

More particularly, the rejection of **Claim 12** asserts that Ala-Laurila discloses receiving a request for a network address from the wireless client as "steps DHCP SOLICIT, figures 4 & 5". The applicant respectfully disagrees with this assertion. While Ala-Laurila does not disclose the DHCP SOLICIT command, Ala-Laurila does include "Dynamic Host Configuration Protocol For IPv6 (DHCPv6) Work in Progress DHCP Working Group 1998, J. Bound and C. Perkins" by reference (*see* Ala-Laurila, col. 3, lines 27-29; hereafter "Bound and Perkins"). Bound and Perkins disclose the DHCPv6 command DHCP SOLICIT as sent by a client to locate a DHCPv6 server (*see* Bound and Perkins, Section 5.3. DHCP Message Types, "SOLICIT (1) A Client sends a solicit message to locate servers"). **Claim 12** does not disclose receiving a request from a wireless client to locate a server; in contrast, **Claim 12** discloses receiving a request for a network address from the wireless client.

The rejection of **Claim 12** further asserts that Ala-Laurila discloses attaching information to the request to indicate that the request originated from a wireless client as a USER ID attached to the DHCP SOLICIT, figures 4 and 5. The Applicant respectfully disagrees with the assertion. The Applicant notes that there is no basis in Ala-Laurila to support the assertion of the rejection that a USER ID is attached to the DHCPv6 DHCP SOLICIT command. Such an attachment is not taught, either expressly or inherently, in Ala-Laurila. For example, FIG.4 and FIG. 5 depict "DHCP SOLICIT + USER ID", such a depiction does not represent an actual combination of the USER ID and the DHCP SOLICIT message. *See* Ala-Laurila, Col. 7, lines 57-59:

> The USER ID and RAND, SRES and Kc authentication information requires separate options/extensions fields where the information is contained in the DHCPv6 protocol.

As discussed above, the DHCP SOLICIT message is not used by a client to request a network address; rather, the DHCP SOLICIT message is used to locate DHCP servers. Furthermore, even if the DHCP SOLICIT message were used to request a network address, the USER ID of Ala-Laurila is not information attached to the request to indicate the request originated from a wireless client. In particular, a USER ID is disclosed by Ala-Laurila at col. 5, lines 56-61 as follows:

> The smart card associated with the user terminal **12**, which may be of diverse designs, provides the user identification (USER ID) as described below in conjunction with FIGS. **4-6** and may be without limitation IMSI or NAI (Network Access Identifier) in accordance with RFC 2486.

More particularly, Ala-Laurila discloses that the user identification will be used to authenticate the user of a device but does not disclose the USER ID will be used for either authenticating or identifying devices. In contrast, the USER ID of Ala-Laurila is constant for the lifetime of the user identifier; the user identifier does not change to reflect changes in the client device. Therefore, the user identifier as disclosed in Ala-Laurila does not change dynamically to indicate that a request originated from a wireless client as the rejection asserts. In contrast, **Claim** 12 does not disclose user information, user identification, or the like, let alone user information attached to a request. **Claim 12** only recites, *inter alia*, information indicating that the request originated from a wireless client. For example, see the specification of the application, page 10, lines 15-18:

> If the origin MAC address is in the database 203, the access point 202 modifies the discover packet at step 306 by inserting data into an optional field of the packet to indicate that the packet originated from a wireless client.

Furthermore, Ala-Laurila discloses the USER ID may be Network Access Identifier (NAI) in accordance with RFC 2486. As is known to those in the art, RFC 2486 discloses that a Network Access Identifier is of the form userid@realm. As can be seen, such a

Network Access Identifier does not contain any information regarding whether or not the client request originated from a wireless device.

Therefore, for at least the reasons set forth above, it is respectfully submitted that **Claims 12, 15, and 19** are patentably distinguishable over Ala-Laurila. The present rejection under 35 U.S.C. §102(e) should be reconsidered and withdrawn.

Rejections Under 35 U.S.C. §102(b)

Claims 9, 11, 17, 21, 22, 24-27, 29 and 30 were rejected under 35 U.S.C. §102(b) as being unpatentable over Lim et al. (U.S. Patent 5,884,024; hereafter "Lim"). The Applicant respectfully traverses the rejection, and requests that this rejection be reconsidered and withdrawn. More particularly the Applicant submits that the rejection does not fulfill all of the requirements of MPEP §2131, which states, in part:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

The rejection of **Claims 9 and 21** asserts that Lim discloses engaging in a negotiation of a secure link with the wireless client at column 7, lines 21-30. Column 7, lines 21-30 of Lim state:

> A preferred method for renewal of an IP address lease by DHCP server system **110** is shown in FIG. 7 and generally designated **700**. Method **700** begins with step **702** where DHCP server system **110** receives a broadcast DHCPREQUEST message from a client system **102**. For the purposes of illustration, it is assumed that the DHCPREQUEST message does not identify a specific DHCP server **110**. Thus, according to the DHCP protocol, the received message is a request from a client system **102** for renewal of an existing lease.

In general, the cited section of Lim is directed to "a preferred method for renewal of an IP address lease by DHCP server system" and not to engaging in a negotiation of a

secure link with the wireless client as in **Claims 9 and 21**. Furthermore, in general, Lim is directed to extending the DHCP protocol to allow a server to check a database to determine whether the requestor of an address should be assigned an address. The DHCP server system of Lim is not concerned with engaging in the negotiation of secure links. That is, the DHCP server system of Lim is not configured to manage links; rather, the DHCP server system of Lim is configured to, *inter alia*, assign internet protocol (IP) addresses to trusted clients and manage lease times and renewals for trusted clients. For example, see column 1, lines

In contrast, **Claims 9 and 21** are directed to a method for controlling access to a network over a secure link. For example, see the specification of the application, page 1, line 7, "a secure link, such as an IPSEC tunnel". As is known to those in the art, IPSEC is an industry standard set of protocols and services used to encrypt data transmission in an IP network. IPSEC is compatible with IPv4 and is included in IPv6. Lim is silent with regard to IPSEC, IPv4, and IPv6, and this is to be expected because, as discussed earlier, Lim is not directed to secure communication on a network.

More particularly, Lim is also silent with respect to a wireless client, and this is also to be expected as Lim is only concerned with assigning addresses to clients regardless of their connection type. That is, Lim is not concerned with securing wireless connections. In contrast, **Claims 9 and 21** recite a secure link with the wireless client. Even if Lim were to disclose a wireless client, as discussed earlier, Lim is silent with regard to a secure link as the DHCP server of Lim does not recite managing secure links.

The engaging of negotiation of a secure link can be found either expressly or inherently in Lim. Furthermore, a wireless client can also not be found either expressly or inherently in Lim. Therefore, the engaging in a negotiation of a secure link with the wireless client can not be found either expressly or inherently in Lim.

The rejection further asserts that if the lease period is determined to be expired, terminating the negotiation, thereby preventing the wireless client from accessing the

network is disclosed in Lim at column 8, lines 38-55. Column 8, lines 38-55 of Lim read as follows:

> ...the lease included in the retrieved record **500** has been renewed by the client system **102**. Step **722** is followed by step **724** where the DHCP server system **110** sends the client system **102** a DHCPACK message. The DHCPACK message informs the client system **102** that the IP address lease has been renewed.
>
> If the DHCP server **110** determines, in step **720**, that the lease included in the retrieved record **500** has expired, method **700** continues at step **726**. In step **726**, the DHCP server system **110** uses the trusted identifier extracted in step **704** to search the trusted identifier database **318**. More specifically, the DHCP server system **110** uses the retrieved trusted identifier to search the trusted identifier index **602** of the trusted identifier database **318**. If an entry is found in the trusted identifier index **602** that matches the retrieved trusted identifier, the DHCP server system **110** retrieves the corresponding record **600**.

More particularly, the cited section of Lim is generally directed to, *inter alia*, a DHCP server sending an acknowledgement to a client that an IP address lease has been renewed, and a DHCP server searching a database containing trusted identifiers and retrieving a match. It is not clear how the cited section of Lim recites determining if a lease period has expired, terminating any type of connection, or preventing any client from accessing any network.

Regardless, as has been discussed earlier, the DHCP server of Lim is not configured to negotiate secure links. Furthermore, also as discussed earlier, the DHCP server of Lim is not able to prevent a client from accessing any network because the DHCP server merely assigns internet protocol (IP) addresses. Even if the cited section were to disclose the DHCP server did not issue an IP address to a client, the connection between such a client without and IP address and the network is not terminated at it is in **Claims 9 and 21**. That is, even though such a client does not have an IP address, it is still connected to the network.

Therefore, for at least the reasons set forth above, it is respectfully submitted that **Claims 9 and 21** are patentably distinguishable over Lim. Furthermore, **Claims 11 and 17** depend from **Claim 9** and are also patentably distinguishable over Lim for at least the same reasons as **Claim 9**. **Claims 22, 24-27, 29 and 30** depend from **Claim 21** and are also patentably distinguishable over Lim for at least the same reasons as **Claim 21**. The present rejection under 35 U.S.C. §103(a) should be reconsidered and withdrawn.

Rejections Under 35 U.S.C. §103(a)

Claims 1-8 and 31-33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Nordman (U.S. Patent 6,061,346; hereafter "Nordman") in view of Garrett, *et al.* (U.S. 20020023160 A1; hereafter "Garrett"). The Applicant respectfully traverses this rejection as the rejection fails to establish a *prima facie* case of obviousness, as set forth in MPEP §2143, which states, in part:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

In general, Nordman is directed to a method for allowing a network-located device to access a private network by authenticating the network-located device in various ways. Furthermore, Garrett is generally directed to a method for managing the forwarding of network packets between networks managed by different service providers. In contrast, **Claim 1** is directed to assigning an address to a wireless client over a secure link using a wireless access point adapted to handle the secure link.

The rejection of **Claims 1, 6, and 31-33** asserts that sending the assigned network address to the wireless client and establishing a secure link is disclosed at

column 7, line 53 to column 8, line 5 of Nordman. Column 7, line 53 to column 8, line 5 of Nordman reads as follows:

> In one embodiment, when the WHI is stored at the HLR **76**, the value stored thereat is provided by way of the line **86** to the SGSN **82**, through the backbone **46** and to the private IP network **14**. The WHI stored at the HLR is forwarded to the SGSN **82** if the authentication procedure confirms the authenticity of the mobile terminal **16**. Thereby, the value of the WHI is authenticated by the authentication procedure performed by the wireless access network. Storage of the WHI at the HLR **76**, or at another portion of the wireless access network, requires an agreement between an operator of the private IP network **14** and the operator of the wireless access network for the secure storage of the value of the WHI at the wireless access network. A separate IP address or DNS (Domain Name Service) name is provided only at the private IP network **14**, and not elsewhere. Thereby, because the IP address and DNS name is provided at the private IP network, the wireless host **32**, when permitted access to the private IP network, becomes a virtual host of the network **14**. The user and host environment of the network **14**, including security and firewalls of the network apply also to the wireless host **32**.

The cited section of Nordman does not recite sending the assigned network address to the wireless client and establishing a secure link as is disclosed in **Claim 1**. For example, see the specification of the application, page 1, line 7, "a secure link, such as an IPSEC tunnel". As is known to those in the art, IPSEC is an industry standard set of protocols and services used to encrypt data transmission in an IP network. IPSEC is compatible with IPv4 and is included in IPv6. In contrast, the cited section of Nordman discloses a wireless host identity (WHI) stored at a home location register (HLR) which is provided to a serving GPRS support node (SGSN) if an authentication procedure confirms the value of the WHI. Once the WHI is authenticated, the wireless host becomes a virtual host of the network that authenticated the wireless host.

More particularly, an authentication procedure is not the equivalent of a secure link. For example, see column 7, lines 38-45 of Nordman:

> While details of the authentication procedure carried out in a GSM communication system can be found in the specification standards of the GSM system, in general, the authentication procedure authenticates, i.e., confirms, that the mobile terminal **16** is permitted to communicate by way of the network infrastructure forming the wireless access network.

If the rejection is asserting that the "line 86" is a secure link, the Applicant notes that no element bearing the number "86" appears in FIG. 1. However, the cited section of Nordman discloses that the "line 86" connects the "HLR 76" to the "SGSN 82" through the "backbone 46" to the "private IP network 14". Such a link is not disclosed as including the wireless host, therefore, even if "link 86" were to be disclosed as a secure link, which it does not, the "link 86" does not include the wireless host. Therefore, "link 86" does not include the wireless host, is not a secure link, and cannot be used for sending an assigned network address to a wireless host as in **Claim 1**.

The rejection further asserts that sending an address of a wireless access point to the wireless client, wherein the wireless access point is adapted to handle the secure link established by the wireless client is disclosed at column 8, lines 12-23 and lines 57-67 of Nordman. Column 8, lines 12-23 of Nordman read as follows:

> ...WHI, and other data, between the private IP network **14** and the wireless access network formed of the network infrastructure. Such authenticated tunneling is performed as the backbone network **46** might be shared by many different operators and security of the backbone can not be assured. For instance, if the HIPN **106** is to be accessed, data is routed by way of a public Internet **108**. The authenticated IP tunneling is performed to authenticate traffic, i.e., communication of data, between the SGSN **82** and the GGSN **92**. Authenticating the traffic routed over the backbone ensures the validity of the value

> of the WHI when the value is received at the GGSN **92**. When, e.g., the HIPN **102** is…

Column 8, lines 57-67 of Nordman read as follows:

> During the attach procedure, the values of the IMSI, the WHI, and other associated subscriber data is downloaded from the HLR **76** to the appropriate one of the MSC/VLR **66** and SGSN **82**. The other appropriate subscriber data includes the address of the private IP network **14**. Addresses of additional private IP networks, such as the HIPN **96**, **102**, and **106** (shown in FIG. 1) may also be downloaded to permit alternate, or second-choice access to an alternate IP network. The HIPN address identifying the private IP network **14**, in one embodiment, is the address of the GGSN, such as the GGSN **92** of the private IP network **14**.

The cited section of Nordman does not disclose a wireless access point, let alone sending an address of the wireless access point to the wireless client. For example, as can be seen from FIG. 1 of Nordman, the wireless access point is the "BTS 52". Nordman defines the BTS at column 6, lines 34-38:

> …a BTS (Base Transceiver Station) **52**. The BTS **52** is operable to generate downlink signals **54** and to receive uplink signals **56** upon an air interface formed of radio links between the remote communication station and the BTS **52**.

The cited section of Nordman does not disclose sending the address of the "BTS 52" to the wireless host, as the "BTS 52" is not recited in the cited section of Nordman. Therefore, it is not possible for the cited section of Nordman to disclose sending an address of the wireless access point to the wireless host.

Furthermore, even if the cited section of Nordman were to disclose sending an address of a wireless access point to the wireless client, which it does not, the cited section of Nordman does not disclose wherein the wireless access point is adapted to handle the secure link established by the wireless client. As discussed previously, the cited section of Nordman does not disclose a wireless access point. The cited section of

Nordman discloses "the authenticated IP tunneling is performed to authenticate traffic, i.e., communication of data, between the SGSN 82 and the GGSN 92." Referring to FIG. 1 of Nordman, it can be seen that the IP tunneling connection is made over the backbone network 92 and the BTS 52 is not disclosed as being included in such a connection.

The rejection further states that Nordman is silent on sending the assigned network address to the wireless client prior to establishing a secure link. The Applicant aggress that Nordman is silent on sending the assigned network address to the wireless client prior to establishing a network link. However, the Applicant does not agree that there is a suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the Nordman with the combination of Garrett (FIG. 9, steps 902-903 and step 904-906) for the stated purpose of allowing authorized use of an IP address and further enhance security of the system.

More particularly, the system of Nordman already includes security, for example, the title of Nordman is "Secure Access Method, and Associated Apparatus, for Accessing A Private IP Network". It is not clear why one of ordinary skill in the art would be motivated to combine Garrett to provide the enhancement of security when a primary concern of Nordman is a secure access method. That is, it is not clear why would one of ordinary skill in the art be motivated to add a "Radius Server 930" from FIG. 9 of Garrett to Nordman, as Nordman already includes a "DHCP Server 920" from Garrett. The "RADIUS Server 930" from FIG. 9 of Garrett is defined in Garrett at paragraph 36 as follows:

> Alternatively, the DHCP server 161 in the service activation system 160 can interact with the registration server 155 using a back-end authentication protocol, e.g. the Remote An Authentication Dial In User Service (RADIUS). See C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)," IETF Network Working Group, RFC 2058 (January 1997), which

> is incorporated by reference herein. The DHCP server can contain a RADIUS client and, thereby, leverage the large RADIUS embedded base used for dial access authentication.
>
> ...
>
> The DHCP server 920 forwards both the challenge and response in a RADIUS_ACCESS_REQ message to a RADIUS server 930 in the selected service network. The RADIUS server 930 either accepts or rejects the RADIUS request and responds accordingly at 906. If the RADIUS request is accepted, the DHCP server 920 sends a DHCPACK message at 907 and the client 910 enters a bound state. If the RADIUS request is rejected, the DHCP server 920 sends a DHCPNACK message which informs the client 910 that the IP address that was allocated has been withdrawn.

That is, the RADIUS Server 930 of Garrett is defined as server providing remote authentication dial in user service. As RFC 2058 has been incorporated by reference into Garrett, RADIUS servers are defined in RFC 2058 at "section 1: Introduction" as follows:

> RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

Nordman already includes such functionality in the form of the Home Location Register (HLR) (*see* Nordman, column 6, lines 55-62, "The HLR 76 includes an authentication center"). Therefore, it is not clear what additional security benefit there would be to including a RADIUS Server of Garrett to Nordman, as Nordman is already capable of providing exactly the same security functionality with the Home Location Register. Therefore, there is no motivation to combine Nordman with Garrett as there is not a case of *prima facie* case of obviousness, as set forth in MPEP §2143.

Even if there were a *prima facie* case of obviousness, as set forth in MPEP §2143 to combine Nordman with Garrett, which there is not, Garrett does not disclose sending the assigned network address to the wireless client prior to establishing a secure link at

FIG. 9 steps 902-907 as the rejection asserts. More particularly, the rejection asserts that authentication is performed at steps 904-906 after the address is assigned and provided to the client at steps 902 and 903.

As has been discussed previously, authentication is not an equivalent operation to establishing a secure link. Garrett is silent with regard to a secure link of any sort, for example, see FIG. 9 and the interaction between 910 HOST, 920 DHCP SERVER, and 930 RADIUS SERVER. No client of any sort is present in FIG. 9 of Garrett. Therefore, FIG. 9 of Garrett is not able to disclose a secure link between any of 910 HOST, 920 DHCP SERVER, or 930 RADIUS SERVER and a client of any sort. However, the silence of Garrett with regard to a secure link with a wireless client is to be expected as Garrett is not concerned with the establishing secure links with clients of any sort. In contrast, Garrett is concerned with the forwarding of network packets to the correct service provider in a set of service providers.

Therefore, without acquiescing to the characterization of the rejected claims, the Applicant respectfully submits that neither Nordman nor Garrett, either singularly or in combination, teaches or suggests the features of independent **Claim 1** or corresponding dependent **Claims 2-8, and 31-33**. The Applicant submits that **Claims 2-8 and 31-33** are patentably distinguishable over the proposed combination of Nordman and Garrett for at least the reasons set forth above due to their dependency upon independent **Claim 1**.

Accordingly, for at least the reasons set forth above, it is respectfully submitted that a *prima facie* case of obviousness has not been established for any of the presently rejected claims. Therefore the present rejection under 35 U.S.C. §103(a) should be reconsidered and withdrawn.

CONCLUSION

All objections and rejections having been addressed, it is respectfully submitted that the present application is now in condition for allowance. Early and forthright issuance of a Notice of Allowability is respectfully requested.

Respectfully Submitted,

Microsoft Corporation

Dated: June 22, 2006

James R. Banowsky, Reg. No. 37,773
(425) 705-3539

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA

CERTIFICATE OF MAILING OR TRANSMISSION
(Under 37 CFR § 1.8(a)) or ELECTRONIC FILING

I hereby certify that this correspondence is being electronically deposited with the USPTO via EFS-Web on the date shown below:

June 22, 2006
Date

Signature

Noemi Tovar
Printed Name